DATAKOM Gesellschaft für Datenkommunikation mbH

Ihr **Lösungspartner** für **IT-Security** und **IT-Messtechnik** für Kommunikationsnetze seit über 30 Jahren

Angriff geglückt – und was jetzt?

Was man tun muss und warum Unternehmen es doch nicht schaffen!

© DATAKOM GmbH

Wer ist Philip Huisgen

- General Manager bei der Datakom
- Studium der BWL an der European Business School
- Promotion an der Wirtschaftsuniversität Wien
- Unternehmensberater bei KPMG, Accenture, CapGemini
- Partner, Geschäftsführer bei kleineren Beratungen

Strategieberatung Go-To-Market Produktportfolio	**Prozessberatung** Organisations- und Prozessentwicklung
Aufbau von Vertriebs-organisationen, -strukturen und -prozessen	**Aufbau von Finanzfunktionen im Unternehmen**

Warum ich mich dieses Themas angenommen habe:

- ❖ IT Security ist kein ausschließliches Thema der IT
- ❖ IT Security ist ein Organisationsthema
- ❖ IT Security ist ein Prozessthema
- ❖ IT Security ist ein Management-Thema

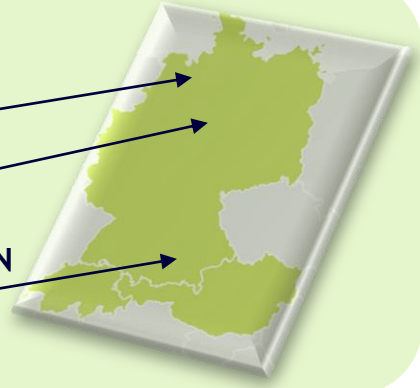
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

DATAKOM in Zahlen

- **1986 gegründet**
- Aktiv in den **Messtechnik, IT Security & Beratung**
- **Hersteller- & lösungsunabhängiger** Partner
- Trendscout bei **Analyse & Auswahl neuer Technologien**

Unsere Standorte:

- ❖ **BREMEN** (Service- & Solution-Center)
- ❖ **BAD PYRMONT** (Vertriebsbüro)
- ❖ **ISMANING b. MÜNCHEN** (Zentrale & Testlabor)



Unsere Referenzen:

17 Mitarbeiter & weitere Freelancer	Zielmärkte **Deutschland Österreich Schweiz**
Derzeit **18 Partner** im Fokus	**26 Standard-Lösungen** im Portfolio

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

IT-Sicherheit ist vielschichtig

PREVENT

Technische und organisatorische Maßnahmen zur Herstellung einer sicheren Umgebung, um Angriffe im Vornhinein weniger wahrscheinlich zu machen.

PROTECT

Vor allem technische Maßnahmen, um aktive Angriffe effektiv und effizient abwehren zu können.

DETECT & RESPOND

Technische und organisatorische Maßnahmen zur sicheren und schnellen Erkennung von Angriffen und der jeweilig sinnvollen Gegenwehr bei gleichzeitiger Vorkehrung der Verhinderung gleicher Angriffe in der Zukunft.

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Kennen Sie den folgenreichsten Datendiebstahl, den es je gegeben hat?

Kennen Sie die böswilligste Cyber-Attacke,
die das Universum je gesehen hat?

SCARIF? Den Namen schon mal gehört?

Die englische Übersetzung
für „1 Schurke“ wäre?

Diesen netten jungen Mann kennen Sie!

Bemerkung:

Hier wurden die Slides aus der vorliegenden Präsentation aus Platzgründen gelöscht.

An dieser Stelle würden 80 Slides folgen, welche die Geschichte vom Film „ROGUE 1“ zusammen-fassen.

ROGUE 1 befasst sich mit einer Cyberattacke (Data Theft).

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Die Leichtigkeit von Angriffen beschleunigt sich…

Alleine ein Aspekt: Über 50% der Angriffe erfolgen durch die eigenen Mitarbeiter…

Accidental Insider		Compromised Insider		Malicious Insider	
Careless behaviour	**Broken Business Process**	**Malware infections**	**Stolen credentials**	**Rogue Employee**	**Criminal actor employee**
Mitarbeiter kennt Sicherheits-standards und Bedrohungs-potenzial nicht und bewegt sich allzu achtlos im IT-Umfeld.	Mitarbeiter um-geht Vorgaben und Policies, um mit Hilfe der IT seine Arbeit zu erfüllen.	Device des Mitar-beiters wurde außerhalb der Sicherheitszone kompromittiert und infiziert ins Netz eingebracht	Login-Daten eines Mitarbeiter wurden gestohlen. Angreifer nutzt diese, um sich Zugang zur IT zu beschaffen.	Ehemals gut-williger Mitar-beiter möchte Daten mit-nehmen, die er für andere Situationen nutzen kann.	Eingeschleuster Mitarbeiter, der von Anfang an zum Ziel hat, dem Unter-nehmen von innen heraus Schaden zuzufügen.

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Die Realität treibt die IT-Security vor sich her…

Drastisch vergrößerte Angriffsfläche

Mehr Endpunkte, mehr virtuelle Maschinen, mehr Mobile-Traffic, mehr Anwendungen, mehr Cloud

Fortgeschrittenere Angriffs-Szenarien

Heutige Attacken sind zielgerichtet, mehrschichtig und umfassen häufig nicht einmal Schadsoftware.

Verfügbarkeit an qualifizierten IT-Security Mitarbeitern

Knappheit an sachkundigen Security Personal zwingt Unternehmen zur vermehrten Automatisierung bei der Bekämpfung von Angriffen.

Ironie dieser Entwicklung: Die Anforderungen an die IT Security explodieren.

Kapazitiver

Flexibler

Automatisierter

Umfassender

Vernetzter

Simpler

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Wo liegen also die Probleme?

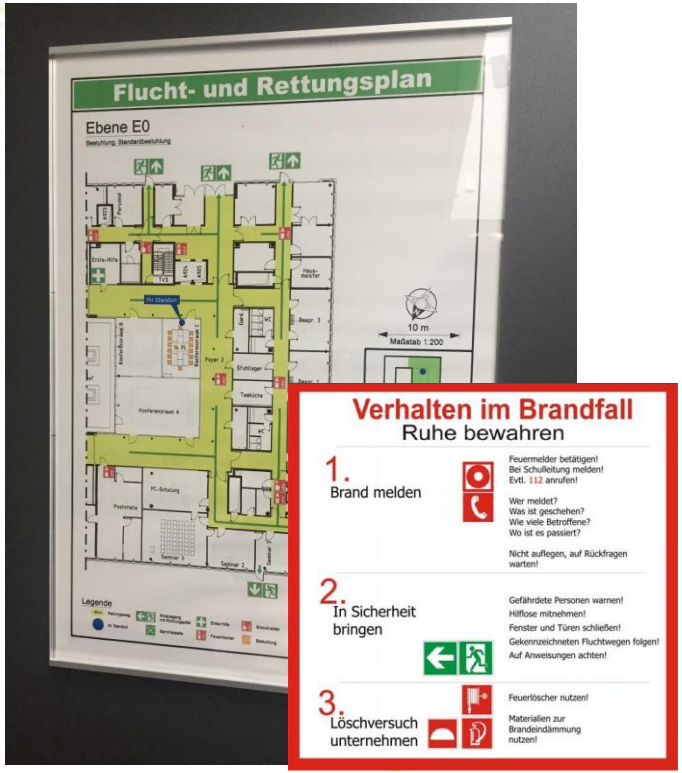
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

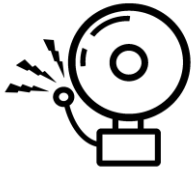
Problem 1:

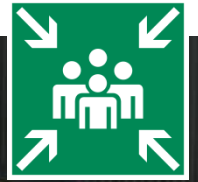
Kein Plan!

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

In Unternehmen gibt es für alles einen Plan.







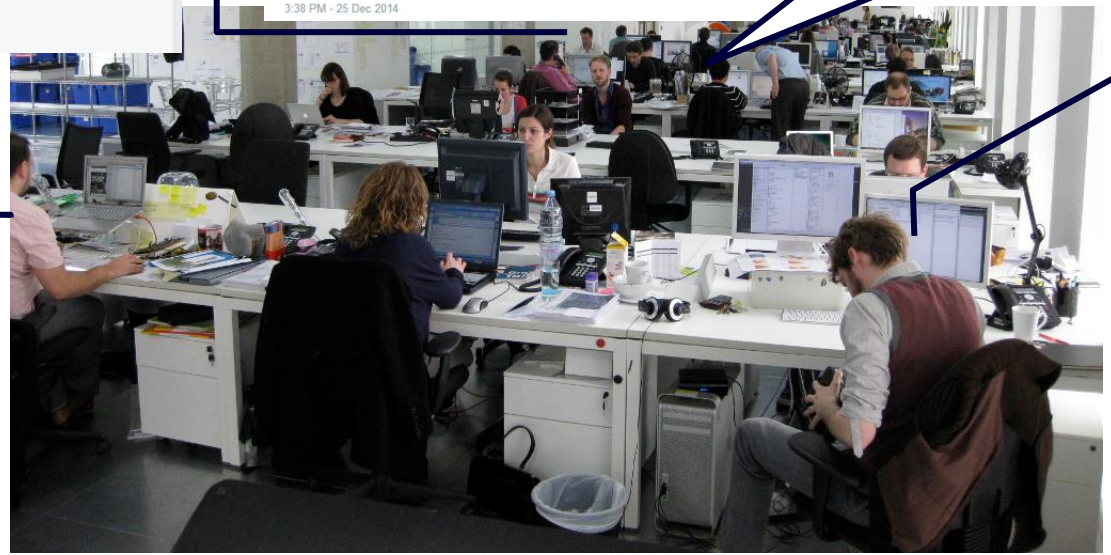
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Aber wie ist es bei einer Cyber-Attacke?

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Ein ganz normaler Verlauf eines Angriffs…

Hier Presseabteilung. Sie sagen, wir sind Opfer eines Cyber-Angriffs? Alles Blödsinn!



Hi Forum,

Wir sind bei XYZ angegriffen worden. Kennt einer von euch „WannaCry“?

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Was es alles braucht

Für die Zeit vor dem Angriff

Verhaltensregeln „Netz-Hygiene“. Trainings, Informationsbroschüren, Notfall-Übungen für die Security Truppe, Angriffs-Simulationen, ISMS

Für die Zeit während des Angriffs

Sicherheitsnotfallplan: Rollen, Ablaufplan, Notfallnummern, Kommunikationsplan. Informationsplan. IR-Krisenteam

Für die Zeit nach dem Angriff

Wiederanlauf: Verantwortungen, Prozess, Rollen, Informationsplan

Angriffsnachbearbeitung: Kommunikation, Schulung, Training, Maßnahmen

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Problem 2:

Schlechte Verbindung!

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

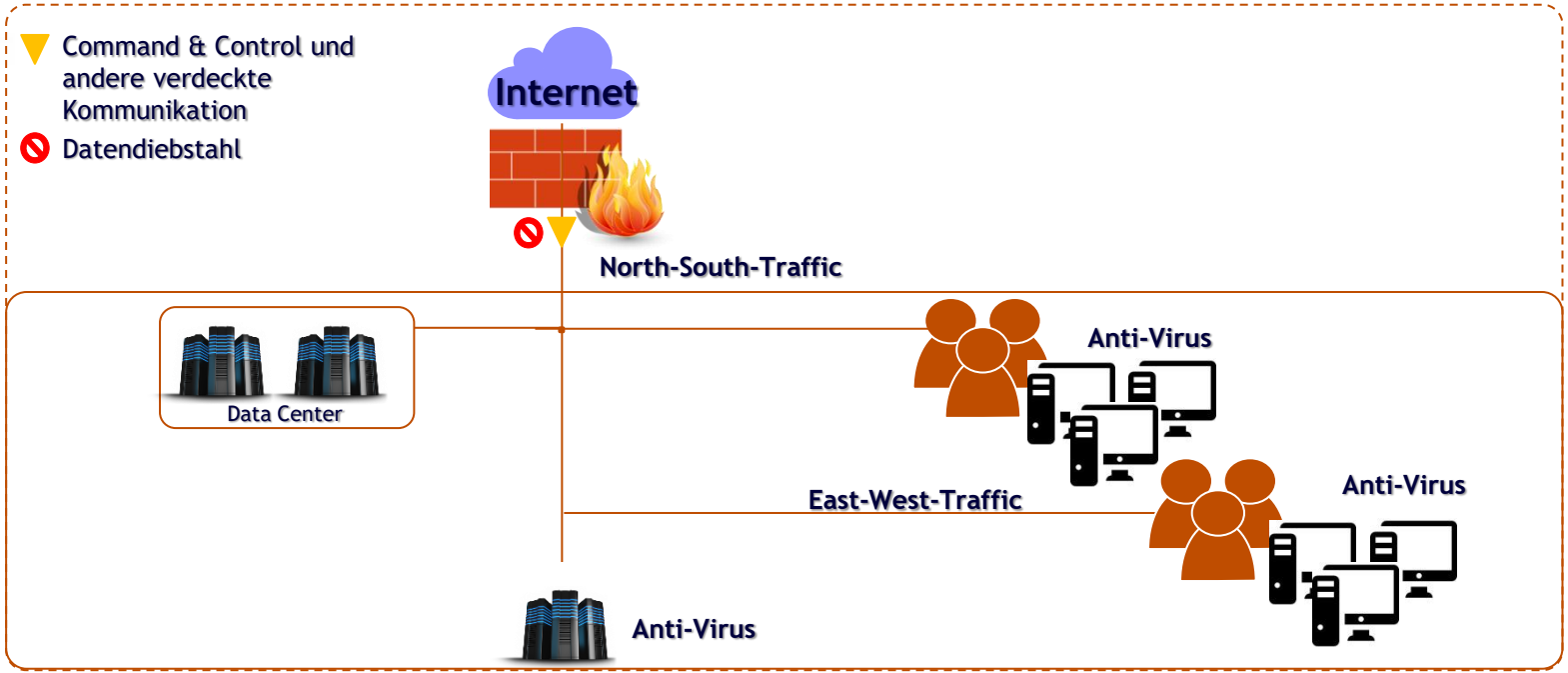
Cyber-Attacken erstmalig sichtbar im Netzwerk

Inline Tools	Out of Band Tools
Real-Time Traffic Inspection	Passive Traffic Inspection
Firewalls, Next Gen Firewalls Intrusion Prevention Systems Data Loss Prevention Systems Unified Threat Management Systems SSL-Decryption Appliance Web Application Firewalls	Intrusion Detection Systems Behaviour Analysis Systems Forensic Tools Data Recording Malware Analysis Tools Log Management Systems Packet Capture Tools

A&O: Optimale, ausfallsichere Anbindung ans operative Netzwerk

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

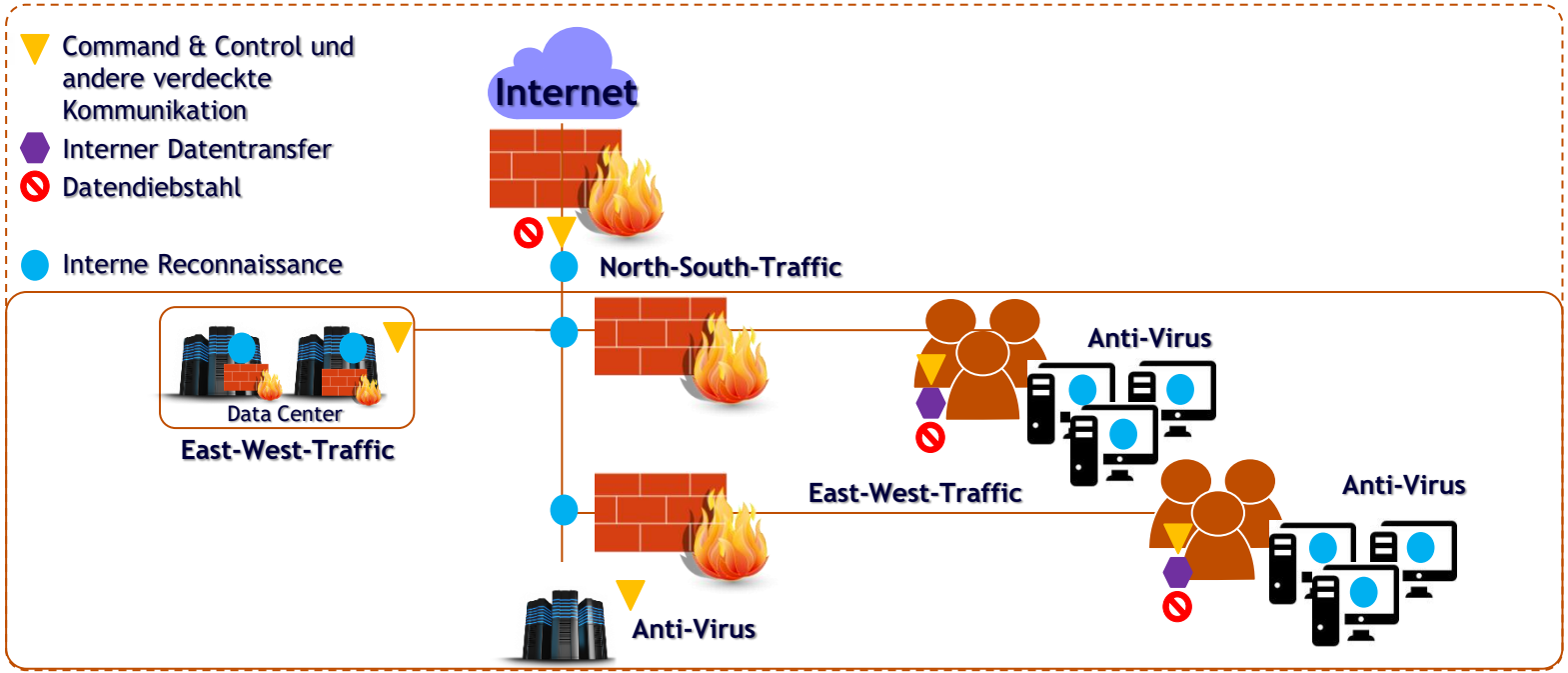
Die einfache Welt der IT-Security…



Netzwerkverkehr: Erster Indikator eines Cyber-Angriffs

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

…wird bei Draufschauen ziemlich kompliziert.



© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

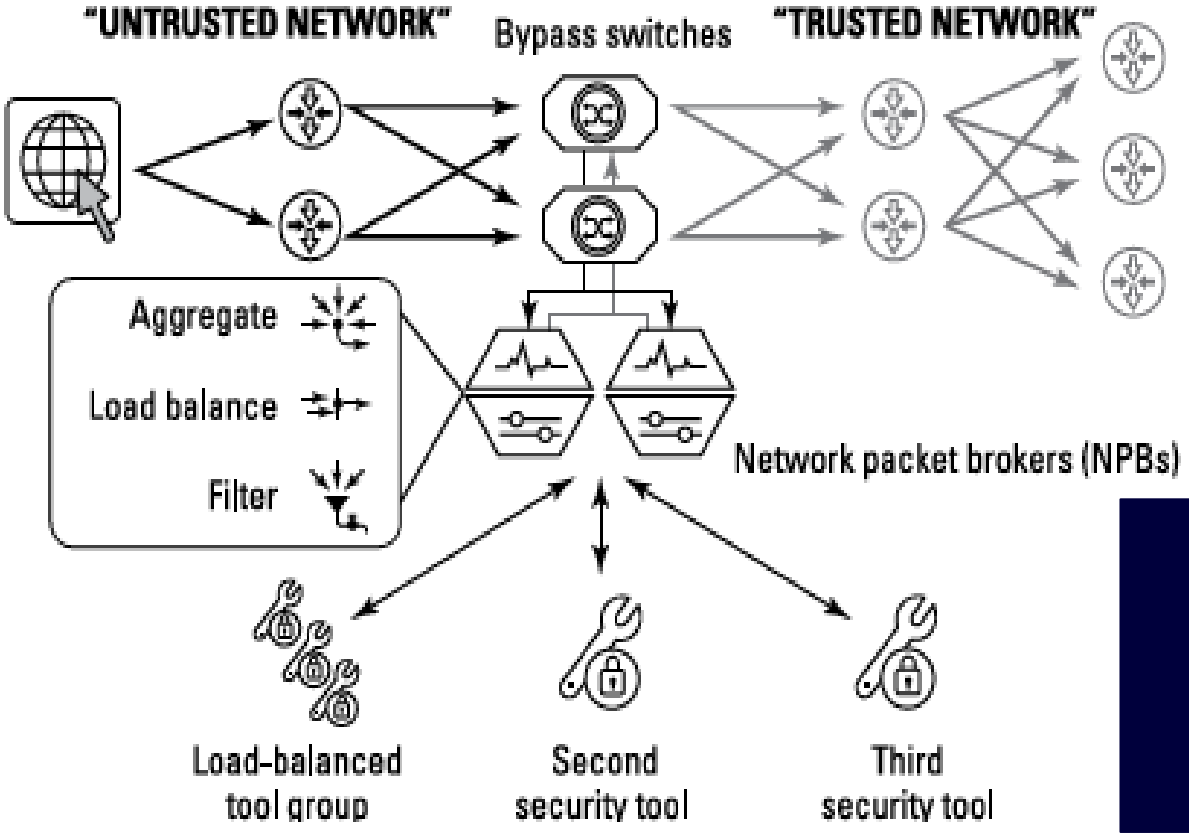
Anforderungen an die Datenströme

Je größer das Netzwerk ist, umso schwieriger wird die Überwachung der Datenströme…

- **Sicherstellung der Netzwerk-Sicherheit**
  - Kontinuierliche, elastische Überwachung der Netzwerk-Sicherheit
- **Anlieferung der richtigen Daten an jeweilige Security Lösung**
  - Unterschiedliche Tools brauchen unterschiedliche Daten
- **Optimierung der Kosten für Überwachungs-Lösung**
  - Monitoring Lösungen extrem teuer, wenn Daten von vielen Network Links zu monitoren sind
- **IT Security Stack aktuell halten, um NW-Verkehr Anforderungen zu managen**
  - Bei Änderungen oder Upgrades der NW-Technologien → Interoperabilität mit Security und Monitoring Lösungen prüfen und anpassen.

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

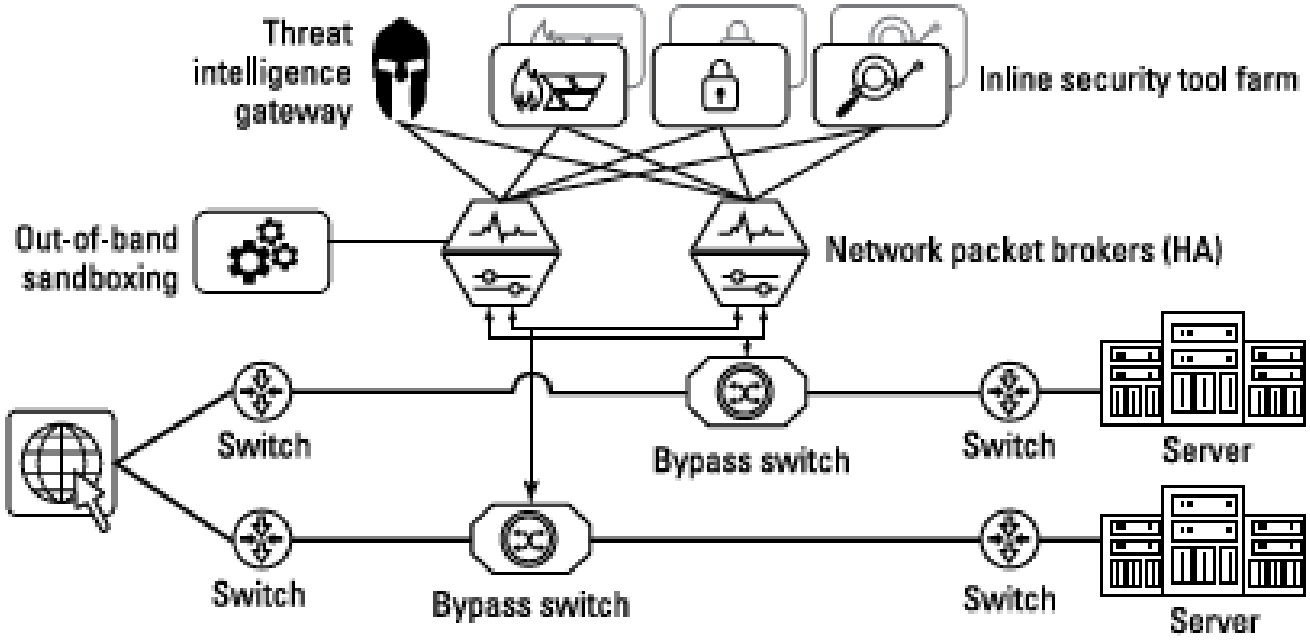
Der Aufbau eines Security Fabrics



- Effizienter Tool-Einsatz
- Betriebssicherheit
- Skalierbarkeit
- Elastizität

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

High Availability Security Fabrics (near-instant failover)



NPB deployed in active-active mode

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Problem 3:

Zuviel Zeug!

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Einige Beispiele in den Domänen…

TECHNISCH	**PREVENT** ISMS, Schwachstellen-Scanner, USB-Port Protection, Multi-factor Authentication	ORGANISATORISCH	User-Training, IT Security-Policies, ISMS, DSMS
	PROTECT Log-Management FW, IPS, Anti-Virus, DLP, Sandboxing		
	DETECT & RESPOND NW-Flow-Mgmt,Log-Inspection Content-Inspection, SIEM Endpoint-Protection und Manipulation		Notfall-Planung SOC-Betrieb, Threat-Hunting CIRT

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Potpourri heutiger Anti-Malware in Unternehmen…

Typische Toolbox des SOC in Unternehmen

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

… hilft kaum, Incident Response effektiv zu realisieren.

Typische Toolbox des SOC in Unternehmen

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Next Evolution Detect & Response
vereinheitlicht 2. Verteidigungslinie

Hewlett Packard Enterprise ArcSight; IBM QRadar; intel Security ESM (Nitro)	Security Information and Event Management
BLUE COAT Security Analytics (Solera); EMC² RSA Network Security Analytics (Netwitness)	Network Security Analytics / Forensics
DIGITAL GUARDIAN Code Green; intel Security DLP (Reconnex); FORCEPOINT Websense DLP; Symantec DLP (Vontu)	Network Content Analysis and DLP
lastline; CYPHORT; TREND MICRO; FireEye	Network Malware Detection
intel Security IPS (Intruvert); Hewlett Packard Enterprise TippingPoint; CISCO SourceFire; IBM IPS (ISS)	Intrusion Prevention Systems
CISCO FirePOWER; FORTINET; paloalto NETWORKS; Check Point SOFTWARE TECHNOLOGIES LTD.	Firewalls

Next Evolution Intrusion Prevention

… erkennt…

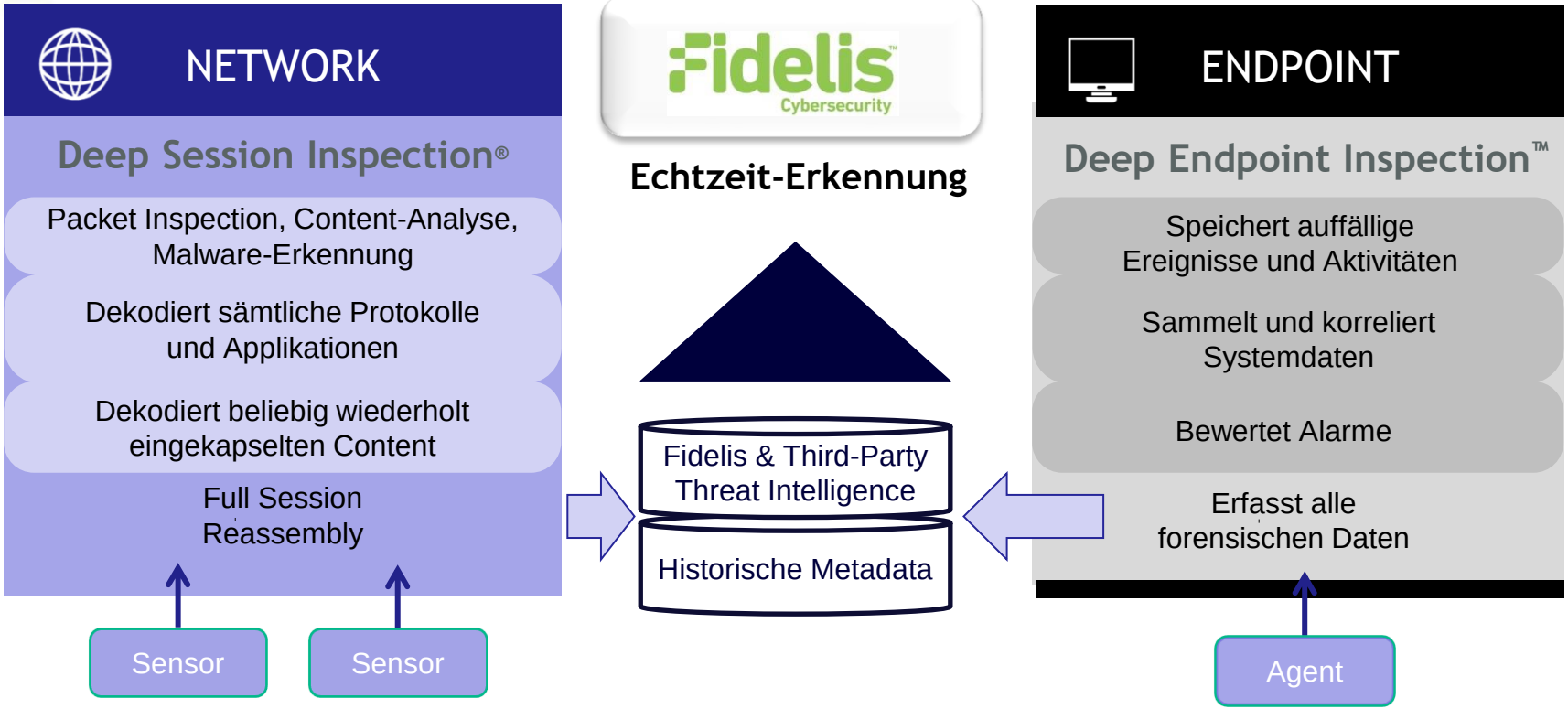
- Malware
- Exploits
- Data theft / DLP

→ Allein dafür braucht man in herkömmlichen Umfeld 3 unterschiedliche Systeme

VECTRA
RSA Fidelis Cybersecurity
Carbon Black.

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

NextEvolution Incident Response Setup-Beispiel



© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

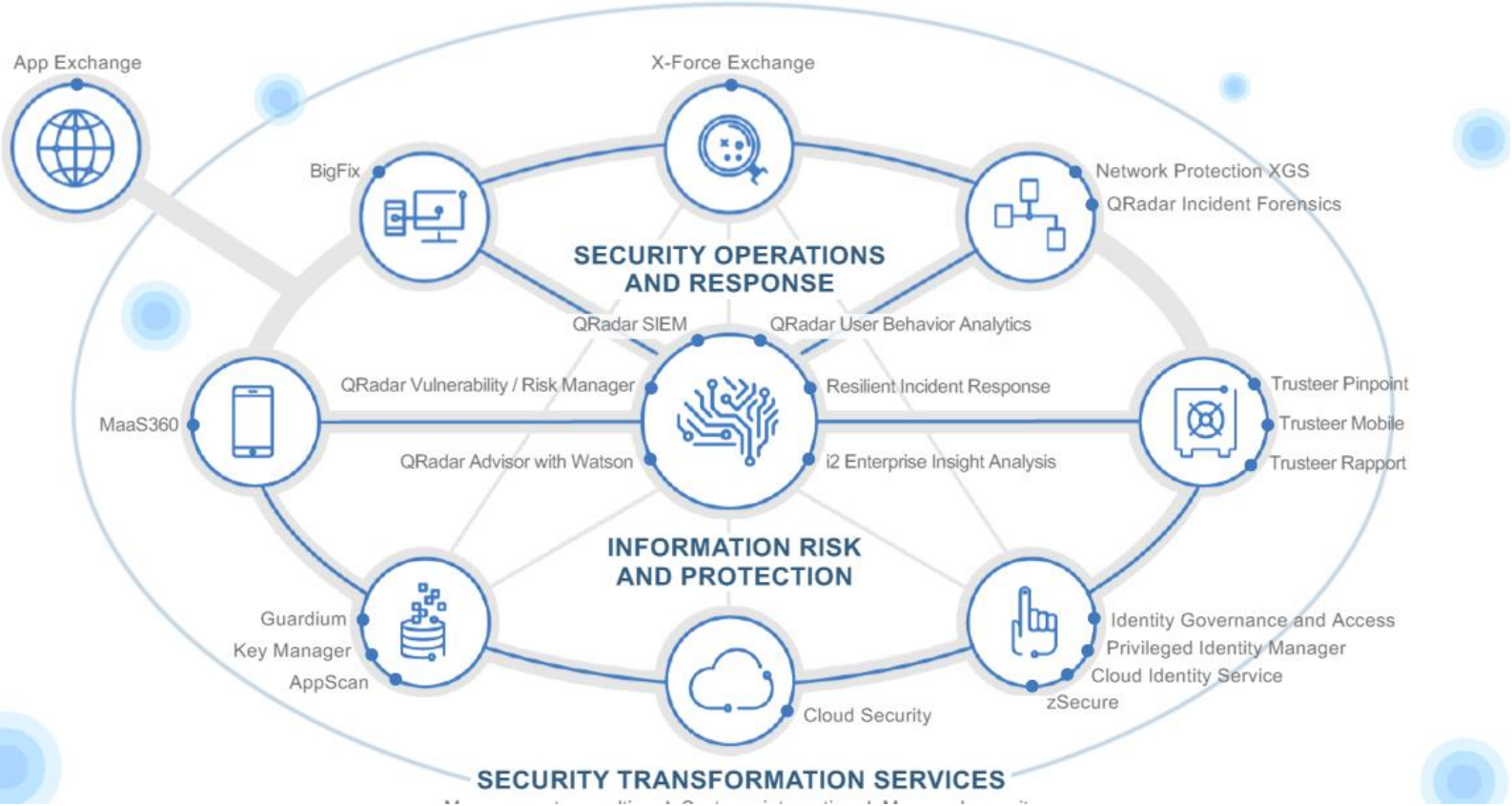
Die Bedeutung von Next Evolution Incident Response ist hoch

Feature	Next-Evo IPS (NEIPS)	Next-Gen Firewall (NGFW)
Firewall	-	x
VPN	-	x
Routing	-	x
URL Inspection	x	x
Packet-Based Signatures	x	x
Malware Analysis / Sandbox Determination	x	x
User Awareness	x	x
Content Inspection	x	-
Endpoint Context	x	-
Rich Alert Forensics	x	-
Historical Metadata for Incident Response	x	-
Application of Threat Intel to Past and Present	x	-
Analytics and Machine Learning	x	x

Wo NE-IPS mehr leistet als eine NGFW

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Die integrierte IBM Welt der Detect & Response



© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Testen Sie Watson

https://www.ibm.com/watson-analytics

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Integriertes, einheitliches Management

- Log Management
- Security Intelligence and Sense Analytics
- Network Activity Monitoring
- Vulnerability and Risk Management
- Network Forensics
- Incident Response

© 2015 IBM Corporation

Security Operations and Response Platform in action

Use advanced analytics to discover and eliminate threats IBM QRadar Security Intelligence	Significantly reduce threat research and response time IBM QRadar Advisor with Watson	Use cyber analysis to hunt for attackers and predict threats IBM i2 Enterprise Insight Analysis	Orchestrate and automate incident response IBM Resilient Incident Response
See, understand, and act on all endpoint threats IBM BigFix	Enhance detection and investigation with threat intelligence IBM X-Force Exchange	Quickly defend your organization with apps and add-ons IBM App Exchange	
Deliver governance, risk and compliance consulting, systems integration and managed security services IBM Security Services			

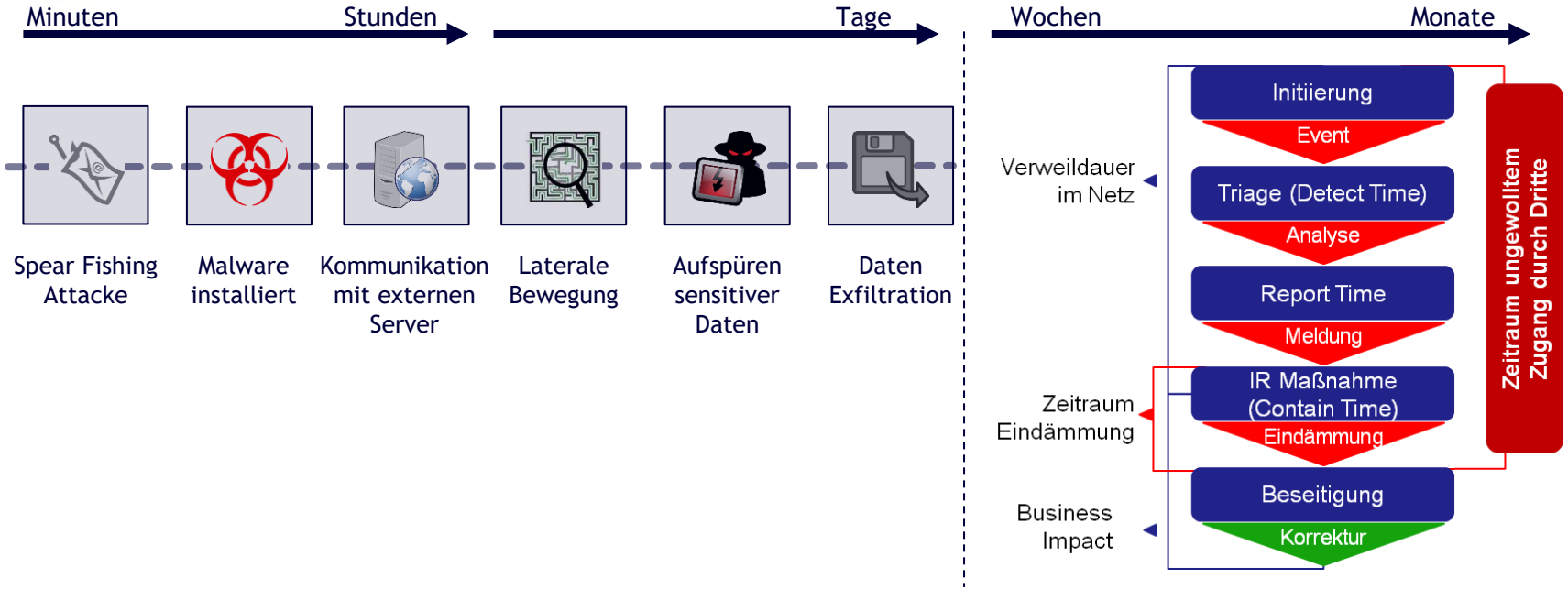
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Problem 4:

Vertrackter Ablauf!

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Angriffe und Gegenwehr stehen in einem Missverhältnis



82% Der Angriffe erfolgreich in MINUTEN

99% Aller Datenverluste innerhalb von TAGEN

64% Erkannt nach MONATEN

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Der typische Bewertungs-Prozess

Prüfung der Warnung und Identifikation des Informationsbedarfs zur Bewertung

Ticket eröffnen, um benötigte Informationen zu erhalten

1. Prüfung der relevanten Informationen (reicht sie aus?)
2. Untersuchung: Wurde verdächtige Netzwerkverbindungen oder Prozesse ausgeführt?

Typischer Tag in einem SOC

Analyse, ob Endpoint kompromittiert wurde

Best Case Scenario

2-5 PT

Manuelles Anpassen von Firewall und IPS Regeln

Manuelle Abklärung ob einziger kompromittierter Endpunkt

System ist potenziell kompromittiert: Manuelles Durchführen Netzwerkisolation, Endpoint-Bereinigung oder neu aufsetzen

Based on customer case studies: Telecom & Energy Customer

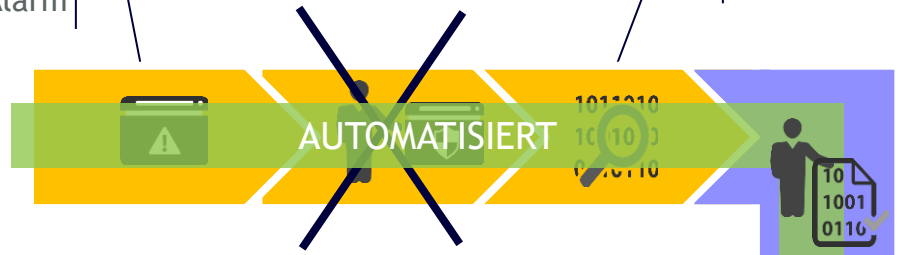
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Der Prozess mit moderner Network/EP Security

Das System erkennt, validiert produziert einen **echten** Alarm

Das System sammelt **automatisch** alle **relevanten Informationen** für die Untersuchung

TYPICAL CASE MINUTES (vs. Days or Weeks)



Sie entscheiden über die notwendigen Maßnahmen und initiieren diese

Das System führt **automatisch Bereinigungsmaßnahmen** durch

Das System **verhindert** automatisch **zukünftige Angriffe** dieser Art

Das System identifiziert sämtliche Bereiche, wo **das Gleiche** in der **Gegenwart und** der **Vergangenheit** geschah und führt Maßnahmen durch.

Based on customer case studies: Telecom & Energy Customer

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Ein schier unüberwindbares Problem?

Kein Plan!

Zuviel Zeug!

Schlechte Verbindung!

Vertrackter Ablauf!

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Das größte Problem ist aber…

Keine Awareness!

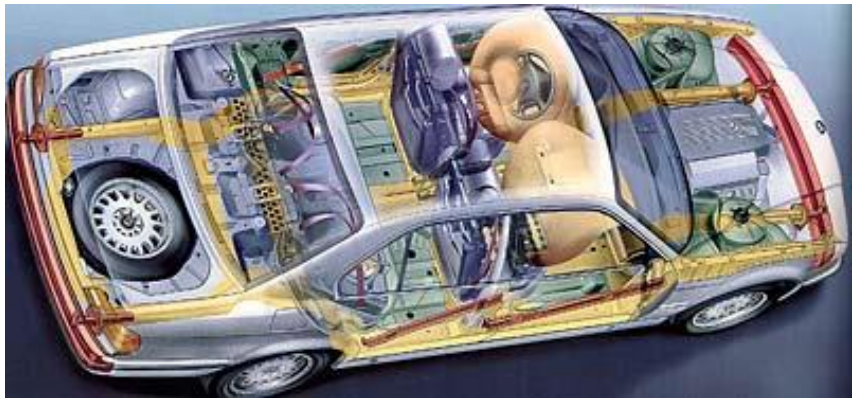
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

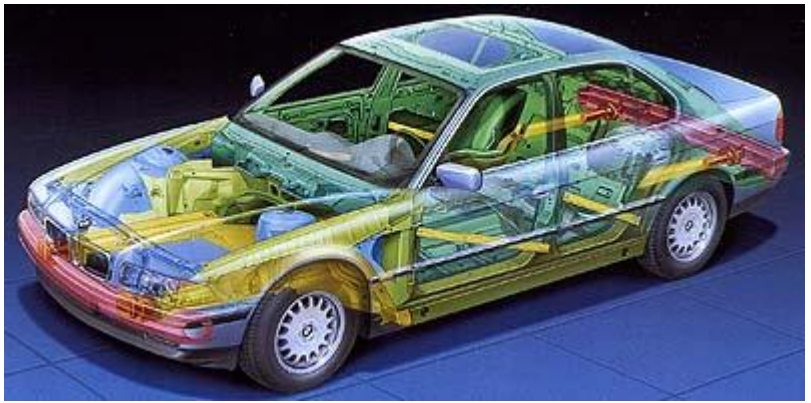
IT Security ist ein Budgetthema

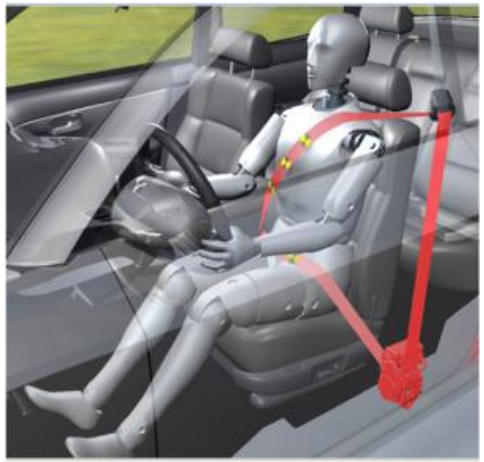
10-20% des gesamten IT-Budgets

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

IT Security ist ein Budgetthema?





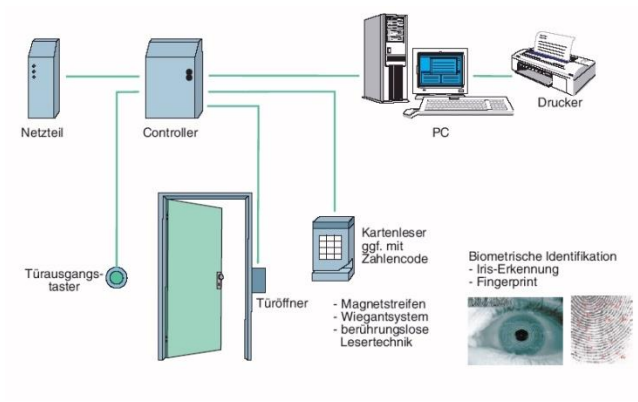


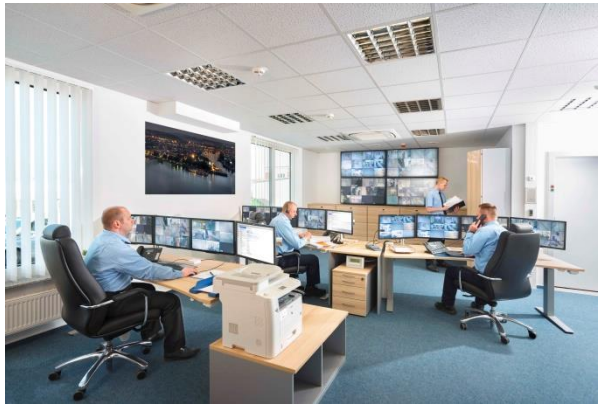
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

IT Security ist ein Budgetthema?

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

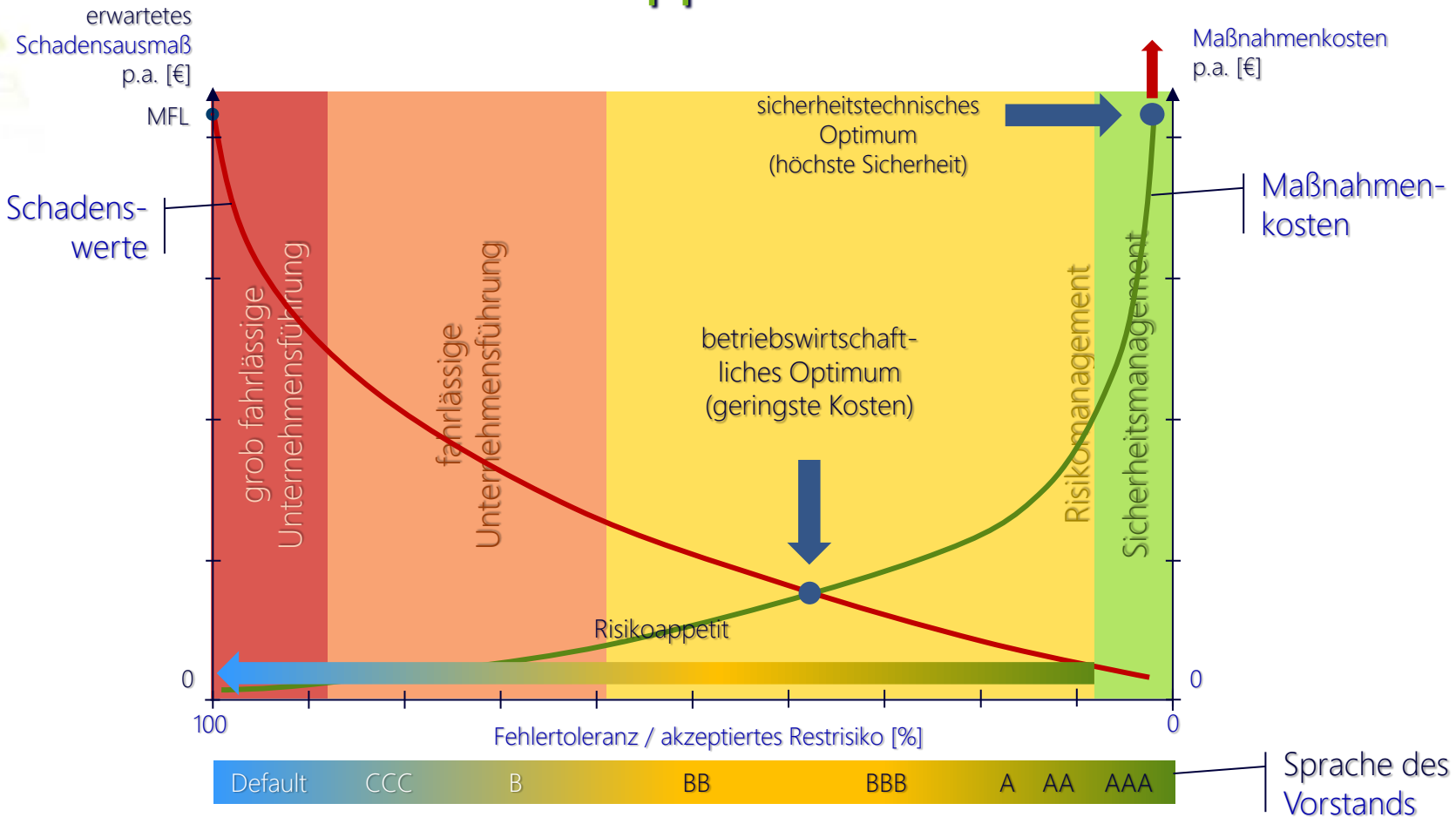
IT Security ist ein Budgetthema?





© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

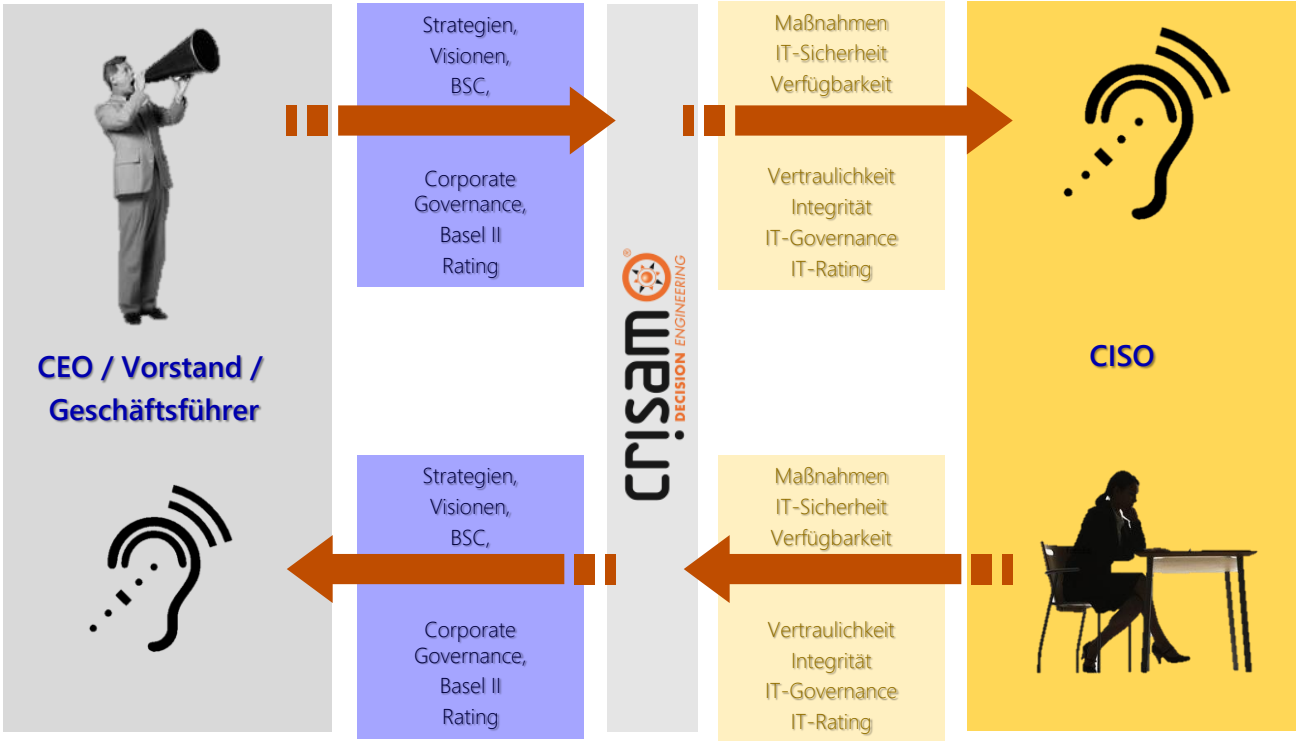
Welcher ist Ihr Risikoappetit?



© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

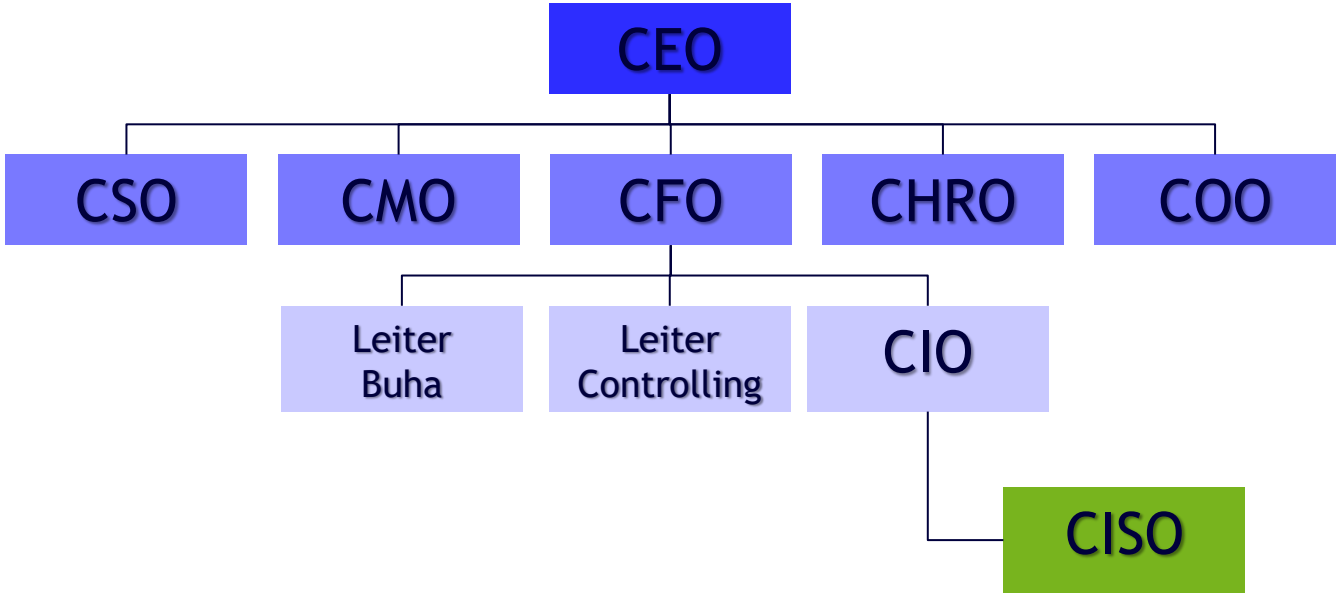
Die Oberste Leitung steuert den Prozess

Der Vorstand / Geschäftsführer muss in seiner Governance-Verpflichtung klare Ziele vorgeben und deren Einhaltung monitoren!



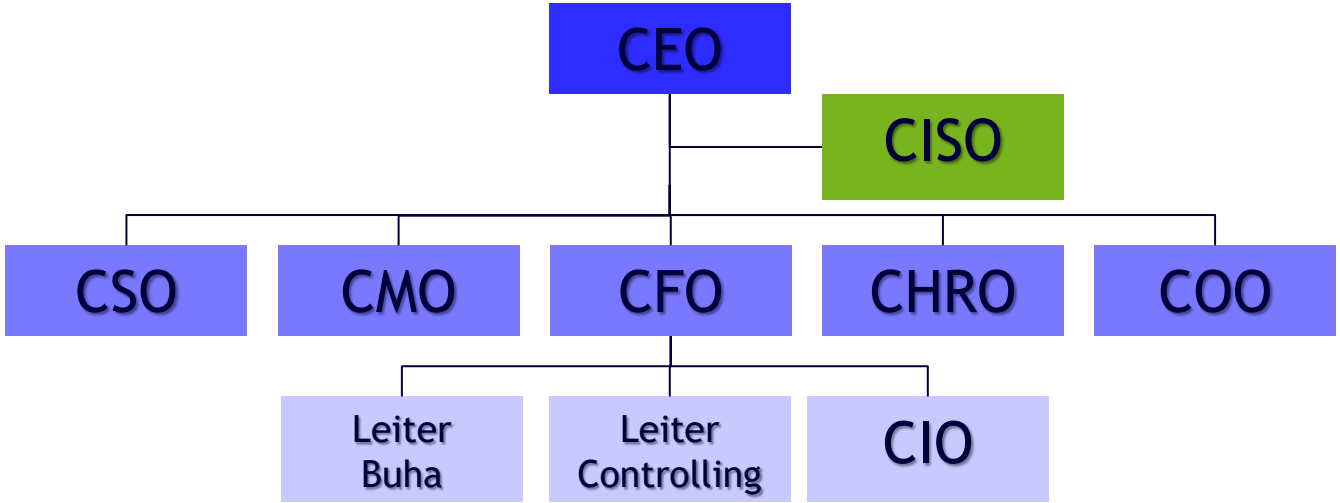
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Und wie sprich der CEO mit dem CISO?



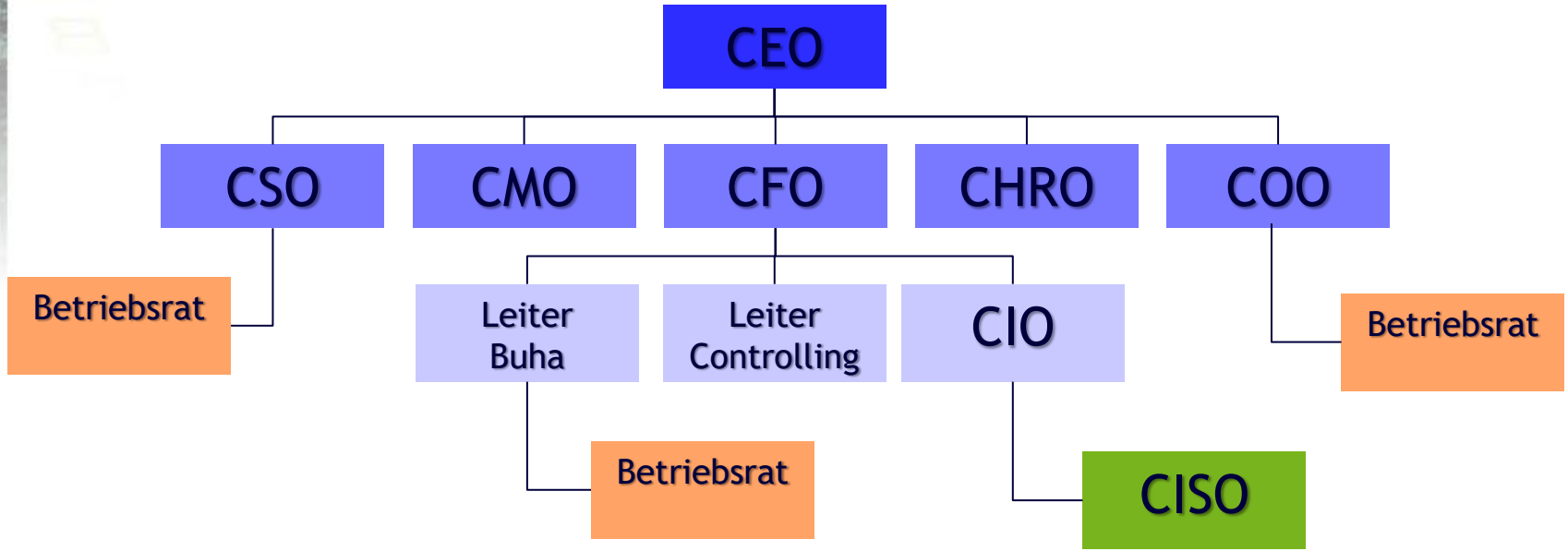
© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Und wie sprich der CEO mit dem CISO?



© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Und wer ist hier der Stärkere?



SSL-Verschlüsselung muss aufgebrochen werden!

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Drei aktuelle Themenfelder für Informationssicherheit die eine gemeinsame Basis bildet!

Informationssicherheit liefert die Basis für ein ISMS nach ISO 2700x, für ein DSMS konform der EU-DSGVO und die Erfüllung des Cyber Security Gesetzes konform der NIS-Richtlinie

ISO 27001

EU-DSGVO

EU-Richtlinie „Netz- und Informationssicherheit“ (**NIS**)
für "**Betreiber unerlässlicher Dienste**"

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Konsequenzen aus der EU-DSGVO

Mehr Eigenverantwortung für den Verantwortlichen im Sinne der EU-DSGVO

1. Informationspflichten (Art. 13 bis 15)
2. Dokumentationspflichten (Art. 30)
3. IT-Sicherheit der Verarbeitung (Art. 32)
4. Einrichtung eines Datenschutzbeauftragten, sofern erforderlich (Art. 37)
5. Datenschutz Folgenabschätzung (Art. 35)
6. Meldepflichten bei Datenschutzverletzung (Art. 33, 34)

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Und wie gehe ich jetzt vor?

Die IT Security Roadmap

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Die „sichere“ IT-Security über die IT-Security Roadmap

Die IT-Security Roadmap strukturiert das Vorgehen zur Erreichung und kontinuierlichen Verbesserung der IT-Security.

IT Roadmap - Bestandteile

- ⇨ Festlegung der IT-Security-Strategie und Risikoappetit
- ⇨ Zielbilddefinition
- ⇨ Bestimmung der Rahmenbedingungen und des Status Quo
- ⇨ Funktionsbestimmung
- ⇨ Policy-Building
- ⇨ Technologiebewertung und -selektion
- ⇨ Organisationsdesign
- ⇨ Identifikation und Schaffung der notwendigen Voraussetzungen
- ⇨ Umsetzungsplanung
- ⇨ Ressourcenzuteilung

- ⇨ Projektdetailplanung
- ⇨ Projektumsetzung und Projektkontrolle

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de

Sie wollen sich im Themenumfeld der IT Security verwirklichen?

Möge die Macht mit Ihnen sein!

Dr. Philip Huisgen
General Manager
Tel.: 0 89 / 99 65 25 - 22
Email: philip.huisgen@datakom.de

DATAKOM Ges. für Datenkommunikation mbH
Lise-Meitner-Str. 1 · 85737 Ismaning

© DATAKOM GmbH · 85737 Ismaning · www.datakom.de